Group Document/Information Retention
&
Destruction Policy

POLICY IMPLEMENTATION CHECKLIST	
Policy Guardian:	Director of Finance & Governance
Author:	Governance Manager
Version number:	1.1
Approved by Chief Executive on:	1 December 2018
Governing Body Approved:	9 December 2018
Effective from:	10 December 2018
Updated:	October 2020
Due for review on:	1 December 2021
Diversity compliant:	Yes
Equality Impact Assessment required:	No
Data Protection compliant:	Yes
Health & Safety compliant:	N/A
Procedure implemented:	Yes
QL system changes made:	N/A
KPIs / reporting arrangements implemented:	Yes
Training Completed:	Yes
Posted on intranet:	Yes
Posted on website:	Yes
Publicity material issued:	
Business Services – Implementation Review:	1 February 2019

This document can also be provided in large print, braille, audio or other non-written format, and in a variety of languages.

1 Introduction

1.1 Information is one of the Caledonia Group ('the Group' comprises of Caledonia, Cordale Bellsmyre Housing Associations) corporate assets; in the course of carrying out its' various functions, the Group collects and processes information from both internal (staff) and external sources (tenants, contractors and other external organisations).

The information collected and documented by the Group can be in several different formats examples of which include, (but are not limited to) communications such as letters, emails and attendance notes; financial information including invoices, statements and reports; legal documents such as tenancy agreements, contracts for supplies and services; and information relating to various types of applications, including forms, plans, drawings, photographs (including CCTV images).

1.2 In this policy, information has been classified as being either personal data which is governed by the requirements of DPA 2018 and GDPR, or business-related information. There may be some business-related information that although has no data protection implications it may still be deemed sensitive (for example if it is of a commercial nature such as completed tender documents) and thus subject to the requirements set out in this policy for retention and disposal.

1.3 For the purposes of this Group Policy, the terms 'document' and 'records' include information in both hard copy and electronic form. In certain circumstances it will be necessary to retain specific documents in order to fulfil statutory or regulatory requirements and also to meet operational needs. Document retention may also be useful to evidence events or agreements in the case of disputes, and also to preserve any information which has historic value.

1.4 The Group must ensure there is robust information governance systems are in place across the Group to identify documents/information for which the appropriate minimum retention period has expired as per the requirements of the Principle in Article 5(1)(a) of the GDPR (as defined below).

1.5 Premature destruction of documents by the Group could result in inability to defend litigious claims raised by individuals or groups; create operational difficulties in relation to effective service delivery or failure to comply with information-related legislations such as those listed in **Section 3.1.**

1.6 It is envisaged that this policy will enable the Group to achieve compliance with the relevant regulatory requirements whilst also enabling searches for information/data requested under legislation to be made as quickly as possible.

1.7 The retention and destruction requirements set out in this policy also apply to information held within the current information systems used across the Group including the housing management system (QL) and its various modules.

1.8 Failure to comply with the retention and destruction requirements set out in the DPA 2018 and GDPR (both as defined below) in relation to personal data could lead to financial penalties, regulatory action, as well as reputational damage for the Group. It is important for the aforementioned reasons that the Group has in place the appropriate systems for the timely and secure disposal of documents and records that are no longer required for business purposes.

2 Scope & Equal Opportunities

2.1 The scope of this policy applies to all Group employees, governing body members, tenant volunteer groups, contractors or delivery partners where they are processing information on behalf of the Group.

2.2 The Group is committed to fairness and equality for all regardless of race, ethnicity, nationality (Gypsies, Travellers and white minority groups are included within these definitions), gender, sexual orientation, marital status, disability, state of health, age, beliefs or religion, appearance, family circumstances or criminal convictions.

2.3 The Group's key aim is to ensure that its' policies and procedures do not create an unfair disadvantage for anyone, directly or indirectly.

3 Relevant Legislation & Group Policies

3.1 The following applicable legislation & Group Policies has been considered in developing this policy:

Legislation

- General Data Protection Regulations (EU) 2016/679 (the GDPR)
- UK Data Protection Act 2018 (the DPA 2018)
- Freedom of Information (Scotland) Act 2002 (FOISA)
- The Environmental Information (Scotland) Regulations 2004 (the EIRs)
- Any legislation that will replace the GDPR in UK law after leaving the European Union.
- Other legislation and guidelines as may be issued from time to time to regulate the use of information systems

Relevant Group Policies

- Group Data Protection Policy
- Group Freedom of Information and Environmental Information Policy
- Group IT Security Policy
- Group Information Risk Policy

4 Group Information Retention & Destruction Policy Objectives

4.1 The key objective of the Group Information Retention & Destruction Policy is to provide the Group with a robust and effective framework that will govern how information/documentation is retained or disposed of within the Group.

Permanent retention of all documents/information is impractical and can lead to the Group breaching legislation in relation to unlawfully retaining personal data/information longer than is necessary. Furthermore, the Group needs to ensure appropriate arrangements are in place to prevent the premature destruction of documents/information that could result in the Group being unable to defend any litigious claims but also not able to comply with the requirements of the GDPR and the DPA 2018 (and the Freedom of Information (Scotland) Act 2002 (FOISA) and Environmental Information (Scotland Regulations 2004 (EIR).

4.2 This Policy also clarifies the different roles and levels of responsibility within the Group in relation to document/information retention and disposal.

4.3 **Appendix A** provides information relating to the Group Retention Schedule, with **Appendix B** providing guidance on the approach used by the Group for document/information disposal.

5 Roles & Responsibilities

5.1 **Group Governing Bodies & Chief Executive**
The Caledonia Management Board and the Chief Executive are responsible for ensuring that the Group meets its legal obligations in relation to information governance. The Management Committee for Cordale, and Bellsmyre also have responsibility for ensuring legal obligations are met for the two respective organisations.

5.2 **Departmental Directors & Operational Managers**
Departmental Directors in accordance with this policy are responsible for determining whether to retain or dispose of specific documents/information within their specific area of responsibility. Directors may where appropriate delegate the operational aspect of this policy to their respective Operational Manager(s).

Directors (or their delegated Operational Manager(s)) should seek legal advice if they are uncertain as to whether the minimum retention periods are prescribed by law, or whether the retention of a document is necessary to protect the Group's position where a potential claim has been identified.

Departmental Directors are also required to ensure that the retention periods set out in Appendix A which are relevant to their service area are kept up to data at all times.

5.3 **Group Data Protection Officer**
The Group Data Protection Officer will be responsible for providing assurance to the Executive Management Team in relation to levels of compliance across the Group in relation to this policy. The Director of Finance & Governance will be responsible for overseeing policy implementation and reporting whilst the Governance Manager will have operational responsibility for ensuring that relevant systems and processes are in place. The Director of Finance & Governance and Governance Manager will perform these duties in consultation with the Group Data Protection Officer as required.

5.4 **Group Staff & Others**
Everyone who works for, or with, the Group has a responsibility for ensuring they fully comply with the guidance set out in this policy in relation to document/information retention **(Appendix A)** and disposal **(Appendix B).**

6 Retention & Destruction of Documents/Information

6.1 This policy supports the Group in demonstrating accountability through the proper retention of documents/information and by evidencing that disposal decisions are taken with proper authority and in accordance with due process.

6.2 The Group Retention Schedule **(Appendix A)** is based on guidance provided by National Housing Federation, Scottish Federation of Housing Associations, and Scottish Council on Archives. The

Group Retention Schedule will be monitored, maintained/updated, and adhered to by those listed in **Section 5** of this policy.

6.3 In circumstances where a document(s)/information has exceed its specific retention period, a review should always be carried out prior to a decision being made to dispose of the document(s)/information. The review must be in accordance with the guidance set out in Appendix B with consideration being given to the documents/information selected for destruction being destroyed in the most appropriate way to ensure compliance with this policy.

6.4 Destruction decisions must **NOT** be made with the sole intent of deliberately denying access or destroying evidence.

6.5 Records of documents/information destroyed will be held by the Governance Team taking advice from the Group Data Protection Officer as required, with details listing the type of document/information destroyed, date of destruction and the director or senior manager who authorised the documents/information destruction.

6.6 No documents/information should be destroyed if they form part of an ongoing external request for information such as a Subject Access Request.

7 Training

7.1 All staff, volunteers, and governing body members will be aware of good practice in data protection and where to find guidance and support for data protection issues including document retention and destruction.

8 Breach of Policy

8.1 Any breaches of this policy may be considered under the Group disciplinary procedures, and may result in disciplinary action being taken, including dismissal.

9 Monitoring and Reporting

9.1 Regular audits will be undertaken to check compliance with the law, this policy and any relevant procedures. Severe risks resulting from data protection compliance requirements relating to document retention and destruction will be considered and monitored within the Group's risk management arrangements.

10 Related Policies & Procedures

10.1 The implementation of this policy will be supported by specific procedural guidance. This will be reviewed and developed on a regular basis to ensure ongoing compliance with legal, regulatory and good practice requirements.

11 Policy Review

11.1 This policy will be reviewed at least every three years by the Group, although changes will be made to the policy during the three-year period if required to meet changes in legislation or any associated requirement.

APPENDIX A

GROUP RETENTION SCHEDULE

Please see separate document.

APPENDIX B

DOCUMENT/INFORMATION DESTRUCTION GUIDANCE

Each of the following questions and guidance listed below should be considered prior to the destruction of any document/information.

1. **Has the document/information been appraised?**
   - Check that the nature and contents of the document/information is suitable for destruction.

2. **Is retention of the document/information required for fulfilling either statutory or regulatory obligations (includes Internal & External Audit, and Insurance purposes)?**

3. **Is the document/information required for evidence purposes?**
   - Keep any documents which may be required for legal proceeding until the threat of proceedings has passed.
   - The limitation period for commencing legal action should also be a key consideration in relation to destructing of documents/information. This is governed by the Prescription and Limitation (Scotland) Act 1973, and the main time limits that apply directly to the Group are:

     1) Contracts or delict (such as negligence) claims (other than personal injury) cannot be brought after five years from the date on which the cause of the action occurred.
     2) Personal injury claims cannot be brought after three years from the date on which the cause of action occurred.
     3) Claims based on provisions contained in documents that are 'under seal' cannot be brought after twelve years from the date on which the cause of action occurred.

4. **Is retention required to meet the operational needs of the Group?**
   - Consider whether the document in question may be useful for future reference, as a precedent or for performance management purposes.

5. **Is retention required because the document/information is of historic interest or intrinsic value?**
   - In most cases this consideration will not be relevant for Group documents/information.
   - If a particular document has a historic or financial value, then consideration should be given to whether it should be retained by the Group, or alternatively, passed to the appropriate external organisation for retention.

6. **Risk Assessment**
   - Selecting the most appropriate destruction method contains an element of risk assessment in terms of the individual carrying out an assessment of the security and costs for destruction of documents/information. These two issues can be summarised in the follow matrix:

Risk Assessment Consideration	**High**	**Medium**	**Low**
How serious would the consequences be for the Group if someone gained unauthorised access to this information?			
What are the cost and time implications of the chosen destruction method?			

The above matrix will not provide a definite answer but will help to guide what are the key considerations are when considering what is the most appropriate method for destruction of documents/information.

7. Destruction of Paper Documents

- If the document does not contain sensitive information it can be destroyed by using the normal waste paper procedure.
- If the document contains sensitive information then it should be disposed of using the confidential waste bins that are located in all the Group's offices in order to avoid breaches of confidence or of the GDPR or DPA 2018.
- The disposal of sensitive information held at scheme locations will be through the use of shredder units held on each site, with a period uplift of the shredded material which will be arranged bythe Governance Team.

8. Destruction of Electronic Documents/Records

- Electronic documents/files (emails) should be deleted when no longer required or have been exceed the timescales set out in the Group retention schedule.
- Electronic documents/information (including emails) should not be deleted if they are subject to a current information request until 60 days after the request has been answered.
- Any queries regarding whether a record is subject to an ongoing information request should be passed to the DPO mailbox in Outlook in the first instance.

9. Destruction of Documents/Information

- Destruction of documents/information listed on the Group Retention Schedule (Appendix A) must be recorded using the Disposal of Records Form (Appendix C).
- All completed Disposal of Records Forms will be held by the Governance Tream for at least 20 years as part of the Group arrangements for ensuring compliance with FOISA and the EIRs. The forms will also be made available to the Group Data Protection Officer to assist with their compliance monitoring activities as required.

APPENDIX C

Disposal of Records Form

Department / Team	
Name of Requester	
Date	
Description of Documents / Information to be Disposed of or Destroyed (including indication of quantity and time period)	
Format (E.g. Paper files / Database records / Electronic files	
Disposal or Destruction?	
Method of Disposal / Destruction (E.g. Self-shred, certificated destruction by contractor, transfer to archive.	

Authorisation Checks (To be completed by Authorised Signatory. Tick to confirm)	
Documents / Information not required as part of current legal proceedings.	
Documents / Information not required in response to current information request.	
Disposal / Destruction accords with Document Retention Schedule.	
Documents / Information not required for any other business related purposes.	
Documents / Information of no historic or financial value.	

Disposal / Destruction Authorisation. (Relevant Operational Manager)	**Name**	**Position**	
	Signature		**Date**
Date of Disposal / Destruction			
Signed			